FCT Fundação para a Ciência e a Tecnologia
Computação Científica Nacional
FCCN

CERT RCTS

How Effective is ASN-Drop?

Carlos Friaças
RCTS CERT, FCT|FCCN
17th October 2019
RIPE 79 Anti-Abuse Working Group

RCTS CERT

- Computer Incident Response Team for the Portuguese Research & Education Network
- Reactive and Proactive services for our constituency base
- Member of RNCSIRT since 2008
  - www.redecsirt.pt
- Member of FIRST since 2011
  - www.first.org
- Certified by Trusted Introducer in 2015
  - Currently under Re-Certification
  - trusted-introducer.org

What is ASN-Drop ?

- A Spamhaus managed list, publicly available
- They list/include ASNs which they think are toxic
  - i.e. where filtering IPs/prefixes is not enough
- A bit like a rating
  - Standard & Poors, Moody's, Fitch, DBRS, …

Disclaimer

- My organisation (FCT|FCCN, AS1930) is **not** using it
- At the CSIRT we consider this to be (free) “intelligence”
- I’m wondering if we should start using it to drop routes
  - i.e. ask the networking department to do it…

How to measure its usefulness?

- Entries still visible in BGP?
  - Go for stat.ripe.net

RIPE NCC
RIPEstat

- ASNs showing up in ROAs?
  - Look at rpki data (from the five RIRs)

- Entries showing up on IXPDB?
  - Query ixpdb.euro-ix.net/en/ixpdb/asns

Which other sources could be useful?

The List…

- www.spamhaus.org/drop/asndrop.txt
- **449** entries
- Syntax: AS ; ISO3166 code ; AS Name/Description

```
; Spamhaus ASN-DROP List 2019/09/29 - (c) 2019 The Spamhaus Project
; https://www.spamhaus.org/drop/asndrop.txt
; Last-Modified: Sun, 29 Sep 2019 02:19:40 GMT
; Expires: Mon, 30 Sep 2019 02:19:40 GMT
```

BGP

- 202 out of 449 entries are visible by RIS

- **44%** of ASNs are still visible

RPKI

- 109.469 ROAs
- 64 out of 449 entries show up in ROAs
- **14%** of ASNs are still part of ROAs

IXPDB

- 39 out of 449 entries show up on IXPDB
- 13 of which at more than one IXP
- **8%** of ASN-DROP entries are declared as IXP members

QUESTIONS

- Should we start dropping routes and incoming packets from these networks?

- Can someone operate a network (and services) if their ASN falls (and remains) on ASN-Drop?

THANKS!
BEDANKT!
DANKE!
MERCI!
OBRIGADO!

CERT
RCTS